Amendments in the Claims

1. (Currently Amended) A network security system, comprising:

a static policy data store having a static policy data attribute;

a dynamic policy data store for tracking a threat level associated with a connection, the dynamic policy data store having a dynamic policy data attribute; and

an authorization enforcement facility (AEF) in communication with ~~said~~ the static policy data store and ~~said~~ the dynamic policy data store and operable to perform a risk-aware analysis of ~~a~~ the connection to determine the threat level associated with the connection based at least in part on the static policy data attribute.

2. (Currently Amended) The network security system of claim 1, wherein ~~said~~ the static policy data store comprises at least one of a constraint, a role, a node-role assignment, a threshold value, a node value, a service value, ~~and~~ or an action value.

3. (Currently Amended) The network security system of claim 2, wherein ~~said~~ the threshold value is inversely proportional to ~~said~~ the node value.

4. (Currently Amended) The network security system of claim 2, wherein ~~said~~ the threshold value is inversely proportional to ~~said node~~ the service value.

5. (Currently Amended) The network security system of claim 1, wherein ~~said~~ the dynamic policy data store comprises a threat level table.

6. (Currently Amended) The network security system of claim 1, wherein ~~said~~ the AEF is further operable to generate a response to ~~said~~ the connection.

7. (Currently Amended) The network security system of claim 6, wherein ~~said~~ the response comprises at least one of blocking the source of ~~said~~ the connection from connecting to an intended destination, altering ~~said~~ the intended destination of ~~said~~ the connection, ~~and~~ or auditing ~~said~~ the connection.

8. (Currently Amended) The network security system of claim 1, wherein ~~said~~ the AEF is further operable to generate a countermeasure.

9. (Currently Amended) The network security system of claim 8, wherein ~~said~~ the ~~wherein said~~ countermeasure comprises an active countermeasure or a passive countermeasure.

10. (Currently Amended) The network security system of claim 1, wherein ~~said~~ the AEF comprises a router, a gateway, a hardware appliance, or a web server.

11. (Currently Amended) The network security system of claim 1, further comprising a firewall in communication with ~~said~~ the AEF.

12. (Currently Amended) The network security system of claim 1, further comprising an intrusion detection system in communication with ~~said~~ the AEF.

13. (Currently Amended) A method comprising:

receiving a static policy data attribute from a static policy data store;

receiving a connection request directed to a node;

~~receiving a dynamic policy data attribute from a dynamic policy data store;~~

determining a threat level associated with ~~whether said~~ the connection request~~ is anomalous~~ based at least in part on ~~said~~ the static policy data attribute ~~and at least in part on~~ said ~~dynamic policy data attribute.~~; and

storing the threat level associated with the connection request as a dynamic policy data attribute in a dynamic policy data store.

14. (Currently Amended) The method of claim 13, further comprising responding to ~~said~~ the connection request.

15. (Currently Amended) The method of claim 14, wherein responding comprises at least one of forwarding ~~said~~ the connection request to ~~said~~ the node; blocking the source of ~~said~~ the connection from connecting to an intended destination, altering ~~said~~ the intended destination of ~~said~~ the connection, ~~and~~ or auditing ~~said~~ the connection.

16. (Currently Amended) The method of claim 13, further comprising updating ~~said~~ the dynamic policy data attribute in ~~said~~ the dynamic policy data store based on a result of ~~said~~ the determination~~ing~~.

17. (Currently Amended) The method of claim ~~13~~16, wherein ~~said~~ the updating comprises increasing ~~a~~the threat level if the connection request is determined to be anomalous.